Case Study

Salesforce

Detecting Salesforce Data Leakage by an Employee

Malicious activities detected

An employee had been approached by one of the company's competitors to extract customer data for competitive advantage. The employee used their permissions within Salesforce, running reports and working with dashboards to extract the requested data over several chunks (in order not to be caught by the DLP rule that sets a threshold for the number of rows extracted via report/dashboard).

User journey analyzed

The sequence of activities performed by an employee during a working session in Salesforce.

Process and assumptions

TrackerIQ learned session profiles for the entire organization, and used these working profiles to detect abnormal/suspicious sessions (i.e. journeys). The assumption is that although export of individual reports is common, sequences of exporting data via reports in a detailed mode, combined with the relevant dashboard activities, are highly unusual.

Industry
Insurance, publicly traded

Application type
SaaS (Salesforce Sales Cloud)

Application usage
The application is the company's main CRM system used by employees to manage customer interactions.

Data analyzed
Audit logs generated by Salesforce and available under its Event Monitoring license. These log files audit user (i.e. employee) activities in Salesforce.

TrackerIQ Analysis Results (over 5 months monitoring of SFDC log data)

- 4 journeys were flagged as suspicious (around 1 per month)
- 1 of the suspicious journeys was of the employee who leaked the data

Even anomalies that were not malicious were important, enabling detection of potential data leakage and requests that employees explain why data was exported.

Customer feedback

Monitoring employee activities and generating alerts about abnormal journeys, even if these journeys are not malicious, is important as a preventive control, given the small number of alerts generated (a few each month). The alternative resulted in true data leakage going undetected, as when the organization had previously implemented a rule to detect reports with large numbers of rows and received tens of alerts a week (false positives).

TrackerIQ Benefits

- Quick initial tuning of the detection model using historical data, including detection of past suspicious activities
- Continuous monitoring of employee journeys to detect ongoing suspicious activities as a preventive control
- An out-of-the-box solution: no need to learn Salesforce logs in-depth and/or to develop rules for Salesforce
- Few alerts per month (around 1-2) allow a focus on truely suspicious activities
- An easy to use investigation tool for the business analyst